ICS 35.030
CCS L 80

# 团　体　标　准

T/TAF 201—2023

# 数据安全管理体系要求

Requirements of data security management system

2023-12-29 发布　　2023-12-29 实施

电信终端产业协会　发布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、泰尔认证中心有限公司、北京通和实益电信科学技术研究所有限公司。

本文件主要起草人：陈思宇、凌大兵、胡越男、范晓杰、薛刚、李杰强、李思桥、刘晓、叶东岳、陈思、汪志、赵昕、王雪、杨光、田崇贤。

# 数据安全管理体系要求

## 1 范围

本文件规定了数据安全管理体系的要求，包括基于ISO管理体系高层架构的数据安全管理要求和配套技术能力要求。

本文件适用于企业组织开展数据安全管理体系的建设，也适用于第三方机构对企业组织的数据安全管理体系进行评价测试工作。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35273—2020 信息安全技术 个人信息安全规范

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**数据安全 data security**

通过采取必要措施,保障数据得到有效保护和合法利用,并持续处于安全状态的能力。

3.2

**个人信息 personal information**

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

［来源：GB/T 35273—2020，3.1］

3.3

**敏感个人信息 personal sensitive information**

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

［来源：GB/T 35273—2020，3.2］

3.4

**个人信息处理者 personal information dealer**

在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

注：与GB/T 35273—2020中的“个人信息控制者”所指一致。

3.5

**去标识化 de-identification**

个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

［来源：GB/T 35273—2020，3.15］

3.6

**匿名化 anonymization**

个人信息经过处理无法识别特定自然人且不能复原的过程。

注：匿名化处理后的信息不属于个人信息。

［来源：GB/T 35273—2020，3.14］

## 4 组织环境

### 4.1 理解组织及其环境

组织应确定与其战略方向及业务活动相关并影响其实现数据安全管理及合规应用的各种外部和内部因素。

组织应在核心业务中识别敏感个人信息、重要数据、核心数据及数据出境的情况，并建立数据安全合规清单。

### 4.2 理解相关方的需求和期望

组织应确定与数据安全管理有关的内外部相关方，并持续监视评价相关方的信息。

组织应识别相关方对于数据安全管理方面的要求和期望，并形成相关方的要求和期望清单。

### 4.3 确定数据安全管理的范围

组织应针对不同业务条线形成不同颗粒度和侧重点的数据安全管理要求，并确定不同业务条线间的数据安全管理边界和适用性，以明确其范围。

在确定范围时，组织应考虑：

a) 4.1中提及的各种内外部因素；

b) 4.2中提及的相关方的要求和期望；

c) 不同业务条线的数据安全需求及特点。

### 4.4 数据安全管理体系

组织应按照本标准的要求，建立、实施、保持和持续改进数据安全管理体系，包括所需的控制及其相互作用。

## 5 领导作用

### 5.1 领导作用和承诺

最高管理者应通过以下方面，证实其对数据安全管理能力的领导作用和承诺：

a） 确保建立了数据安全战略和目标，并与组织的战略方向一致；

b） 确保数据安全管理要求融入组织的业务过程；

c） 促进使用过程方法和基于风险的思维；

d） 确保数据安全管理体系所需的资源是可获得的；

e） 确保数据安全管理能力实现其预期结果；

f） 指导并支持相关人员为数据安全管理体系的有效性作出贡献；

g） 推动持续改进数据安全管理体系；

h） 支持其他相关管理者在其职责范围内发挥领导作用。

### 5.2 方针

最高管理者应制定、实施和保持数据安全管理方针，该方针应：

a） 满足4.1和4.2中提及的组织内外部因素、相关方需求和期望；

b） 符合组织的战略发展方向及数据战略规划；

c） 为建立数据安全目标提供框架。

方针应保持成文信息，并在组织内得到沟通、理解和应用。

### 5.3 组织的岗位、职责和权限

最高管理者应确保组织与数据安全管理相关的职责、权限得到分配和沟通。

最高管理者应分配职责和权限，以：

a） 确保数据安全管理体系符合本标准的要求；

b） 确保数据安全主要负责人向最高管理者报告数据安全管理体系的绩效；

最高管理者应确保组织按附录A中组织机构的相关要求建立数据安全组织架构，明确岗位职责，确定数据安全主要负责人。

## 6 策划

### 6.1 应对风险和机遇的措施

组织在策划数据安全管理体系时，应考虑4.1所提及的因素和4.2所提及的要求，并确定需要应对的数据安全风险和机遇。

组织应策划：应对这些风险和机遇的措施；如何在数据安全管理能力过程中整合并实施这些措施；如何评价这些措施的有效性。

### 6.2 数据安全风险评估

组织应建立数据安全风险评估过程，过程应包括：

a） 制定数据安全风险准则；

b） 实施数据安全风险评估活动；

c） 开展数据安全风险的分析及评价。

组织应制定并维护数据安全风险准则，准则应包括：

a） 明确数据安全风险评估原则；

b） 明确数据安全风险评估的实施流程；

c） 明确数据安全威胁及脆弱性分类；

d） 明确风险责任人。

组织应依据数据安全风险评估准则定期开展数据安全风险评估活动，风险评估活动应包括：

a） 识别数据资产及数据应用场景；

b） 识别威胁、脆弱性及已有安全措施。

组织应依据数据安全风险准则开展数据安全风险的分析及评价，应包括：

a） 依据数据资产、威胁及脆弱性等相关影响因素确定安全事件发生可能性；

b） 依据数据资产及脆弱性程度确定安全事件影响程度；

c） 依据安全事件发生可能性及安全事件影响程度，确定数据资产在相应场景下的安全风险项；

d） 综合各场景中的风险项，确定总体安全风险。

### 6.3 数据安全风险处置

组织应实施数据安全风险处置过程，过程应满足：

a） 建立数据安全风险处置计划，并按计划实施数据安全风险处置活动；

b） 根据安全风险及相关分析评价结果，确定需进行数据安全风险处置的风险项；

c） 将6.3b）确定的风险项所采取的控制措施与附录A中的控制进行比较，并验证没有忽略必要的控制。

### 6.4 数据安全目标及其实现的策划

组织应在相关职能和层级上建立数据安全目标。

数据安全目标应：

a） 基于组织的数据安全总体策略，与数据安全方针保持一致；

b） 可测量（如可实现）；

c） 考虑适用的数据安全法律法规、数据安全风险及相关方的要求；

d） 得到监视及沟通；

e） 适时更新。

组织应保持有关数据安全目标的成文信息。

策划如何实现数据安全目标时，组织应确定：

a） 要做什么；

b） 所需资源；

c） 由谁负责；

d） 何时完成；

e） 如何评价结果。

**注：**数据安全目标及战略规划具体控制措施参考附录A数据安全战略规划。

## 7 支持

### 7.1 资源

组织应确定并提供建立、实现、维护和持续改进数据安全管理体系所需的资源。

### 7.2 能力

组织应：

a） 确定在组织控制下从事会影响组织数据安全绩效的工作人员的必要能力；

b） 确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c） 适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；

d） 保留适当的文件化信息作为能力的证明。

注：教育培训的具体控制措施见附录A人员管理。

### 7.3 意识

组织应确保在其控制下的工作人员意识到：

a） 数据安全管理方针；

b） 其对数据安全管理体系有效性的贡献，包括改进数据安全管理体系绩效的益处；

c） 不符合数据安全管理体系要求的后果。

注：建立意识的具体措施可参考附录A人员管理中的责任保持部分。

### 7.4 沟通

组织应确定与数据安全管理体系相关的内部和外部的沟通需求，包括：沟通内容、沟通时机、沟通对象、沟通方式等。

### 7.5 文件化信息

组织的数据安全管理体系应包括：

a） 本标准要求的文件化信息；

b） 为数据安全管理体系有效性，组织所确定的必要的文件化信息。

注：组织的文件化体系内容见附录A制度保障。

### 7.6 文件化信息的创建和更新

组织创建和更新数据安全管理体系文件化信息时，组织应确保适当的：

a） 标识和描述（如标题、日期、作者或引用编号）；

b） 格式（如语言、版本、图表）和介质（如纸质或电子）；

c） 对适宜性和充分性的评审和批准。

### 7.7 文件化信息的控制

应控制数据安全管理体系和本标准所要求的成文信息，以确保：

a） 在需要的场合和时机，均可获得并适用；

b） 予以妥善保护（如防止泄密、不当使用或损失）。

为控制文件化信息，适用时，组织应强调以下活动：

c） 审批、分发、访问、检索和使用；

d） 存储和保护，包括保持可读性；

e） 控制变更（如版本控制）；

f） 保留和处理。

对于组织确定的策划和运行数据安全管理体系所必须的来自外部的成文信息，组织应进行适当识别，并予以控制。

## 8 运行

### 8.1 运行的策划和控制

为满足数据安全的要求，并实施第6章所确定的措施，组织应通过以下措施对所需的过程进行策划、实施和控制：

a) 建立附录A所列明的数据安全管理体系控制措施，包括数据安全组织机构、人员管理、制度保障、数据安全战略规划、数据资产管理、分类分级、权限管理、安全审计、合作方管理、应急响应、举报投诉相关管理控制措施；

b) 按照相关控制措施对实际的实施过程进行控制。

应在必要的范围和程度上保留文件化信息，以确信相关措施已按照计划得到执行。

### 8.2 数据全生命周期管理

组织应按附录A建立数据全生命周期的管理，明确针对数据采集、数据传输、数据存储、数据使用、数据开放共享及数据销毁的相关控制措施。

## 9 绩效评价

### 9.1 监视、测量、分析和评价

组织应评价数据安全绩效以及数据安全管理体系的有效性。

组织应确定：

a) 需要被监视和测量的内容，包括数据安全管理体系的控制措施和目标；

b) 适用的监视、测量、分析和评价的方法，以确保得到有效的结果。

### 9.2 内部审核

组织应按计划的时间间隔进行内部审核，确定数据安全管理体系：

a) 是否符合组织自身的管理体系要求及本标准的要求；

b) 是否得到有效实现和维护。

组织应依据安全审计的相关要求，实施内部审核。

注：安全审计的具体控制措施见附录A安全审计。

### 9.3 管理审核

最高管理层应按计划的时间间隔评审组织的数据安全管理体系，以确保其持续的适宜性、充分性和有效性。

管理评审应考虑：

a) 以往管理评审提出的措施的状态；

b) 与数据安全管理体系相关的外部和内部事项的变化；

c) 有关数据安全绩效的反馈，包括以下方面的趋势：

1） 不符合和纠正措施；

2） 监视和测量结果；

3） 审核结果

4） 数据安全目标完成情况。

d) 相关方反馈；

e) 数据安全风险评估结果及应对措施的状态；

f) 持续改进的机会。

管理评审的输出，应包括与持续改进机会相关的决定，以及变更数据安全管理能力的任何需求。

管理评审结果，应保留成文信息。

## 10 改进

### 10.1 不符合及纠正措施

当发生不符合时，组织应：

a） 对不符合作出反应，适用时：

1） 采取措施，以控制并予以纠正；

2） 处理后果。

b） 通过以下活动，评价是否需要采取措施，消除产生不符合的原因，以防止不符合再发生，或在其他地方发生：

1） 评审不符合；

2） 确定不符合的原因；

3） 确定类似的不符合是否存在，或可能发生。

c） 实施任何需要的措施；

d） 评审任何所采取的的纠正措施的有效性；

e） 必要时，对数据安全管理体系进行变更。

纠正措施应与不符合的影响相适合。

不符合的纠正过程，应保留成文信息。

### 10.2 持续改进

组织应持续改进数据安全管理体系的适宜性、充分性、有效性。

# 附 录 A
（规范性）
数据安全管理体系控制措施

数据安全管理体系控制措施见表A.1。

表A.1 数据安全管理体系控制措施

| 控制措施 | | 内容 |
|---|---|---|
| 组织机构 | 数据安全组织架构 | （管理措施）应建立数据安全管理组织架构，架构应至少包括决策层、管理层、执行层和监督层，其中决策层应由机构最高管理者或授权代表担任领导，并明确其责任与权力。 |
| | 岗位职责 | （管理措施）应基于数据安全管理组织架构设立相关职能岗位，明确岗位人员要求、职责划分。职能岗位应包括但不限于数据资产管理、分类分级、权限管理、安全审计、合作方管理、应急响应、教育培训、举报投诉等方面。 |
| | 主要责任人 | （管理措施）组织应明确数据安全主要责任人，责任人履行职责包括但不限于：<br>a） 组织建立数据安全管理体系；<br>b） 监督数据安全管理体系的运行、保持和改进；<br>c） 组织开展数据安全风险评估活动；<br>d） 监督数据安全风险处置活动的实施；<br>e） 按要求向有关部门报告数据安全保护和事件处置情况。 |
| 人员管理 | 责任保持 | （管理措施）应明确数据安全追责机制，定期对责任部门和岗位进行安全检查，形成检查报告。 |
| | | （管理措施）应与接触敏感个人信息、重要数据、核心数据的关键岗位人员签署安全责任书，并在其调离岗位或解除劳动合同前，与其签署保密协议。 |
| | | （管理措施）应对接触敏感个人信息、重要数据、核心数据的关键岗位人员进行背景调查，调查应涉及法律法规、行业道德准则、专业能力等方面内容。 |
| | | （管理措施）应建立明确的奖惩制度体系并在组织内部进行宣贯以确保相关人员建立数据安全意识。 |
| | 教育培训 | （管理措施）组织应制定数据安全管理相关岗位人员培训计划，并按计划定期开展数据安全教育培训，培训内容应至少包括：法律法规、政策标准、合规管理、应急响应、专业知识及技术工具应用、安全意识等。 |
| | | （管理措施）组织数据安全教育培训可采取线下集中授课或线上培训形式，培训时长宜每年度不少于20课时，每课时不少于30分钟，培训人员应通过相应的考核评定，并留存培训考核记录。 |
| 制度保障 | 制度体系 | （管理措施）组织应建立完整的制度体系，应至少包括以下四个层级：<br>a） 第一层级，应建立包括数据安全管理手册、数据安全战略规划等在内的纲领性文件，相关文件应覆盖组织的数据安全管理方针、安全目标、安全原则；<br>b） 第二层级，应制定包括数据安全管理制度、办法和标准，相关文件应覆盖数据资产管理、分类分级、风险评估、权限管理、安全审计、应急响应、教育培训、举报投诉等方面内容；<br>c） 第三层级，针对第二层级的文件应制定具体的操作流程、规范及作业指导文件， |

表 A.1　数据安全管理体系控制措施（续）

| 控制措施 | | 内容 |
|---|---|---|
| 制度保障 | 制度体系 | 并形成相应的配套模板；<br>d)　第四层级，在相关管理制度执行过程中应形成相应的计划、表格、报告、运行/检查记录、日志文件等。 |
| 数据安全战略规划 | | （管理措施）应明确符合组织数据战略规划的数据安全总体策略，明确数据安全目标、方针和原则。 |
| | | （管理措施）应明确组织数据安全战略规划路径，包括各阶段目标、任务、工作重点等，并保证其与组织的实际业务规划相适应。 |
| 数据资产管理 | | （管理措施）组织应建立数据资产管理制度，明确数据资产登记机制，建立数据资产清单，明确数据资产相关方。 |
| | | （管理措施）组织应定期梳理数据资产，并根据数据资产范围的变化更新数据资产清单。 |
| | | （技术措施）组织应建立数据资产识别技术手段，定期对相关平台系统进行梳理，明确数据资源内容、数据量、类别分布等信息，应具备发现敏感个人信息、重要数据、核心数据的技术能力。 |
| 分类分级 | | （管理措施）组织应建立数据分类分级制度，明确数据分类分级的原则、方法和手段。 |
| | | （管理措施）组织应对其数据资产实施分类分级管理工作，并形成数据分类分级清单；分类分级清单应覆盖组织全部数据资产。 |
| | | （技术措施）组织应根据组织的业务特点和外部合规要求，对不同类别和级别的数据建立差异化的权限控制、加密脱敏、存储防护等安全保障措施。 |
| 权限管理 | | （管理措施）组织应制定权限管理办法，明确对涉及数据处理相关的系统和数据库的身份标识与鉴别、访问控制及权限的分配、变更、撤销等管理要求。 |
| | | （管理措施）应明确系统平台及数据库的用户账号权限审批和操作流程，形成并定期更新权限分配表。 |
| | | （管理措施）应按最小够用等原则对用户账号权限进行分配。 |
| | | （管理措施）应定期审核数据访问权限，及时清理回收过期账户权限。 |
| | | （管理措施）涉及数据重大操作的（如数据批量复制、传输、处理、开放共享和销毁等），组织应采取多人审批授权或操作监督，并实施日志审计。 |
| | | （技术措施）关键系统和数据库应具备访问控制功能，具备对用户权限进行分配的能力。 |
| 安全审计 | | （管理措施）组织应建立数据安全审计相关制度规范，明确审计对象、审计内容、实施周期、审计流程等要求，明确数据安全审计过程中各相关方的职责。 |
| | | （管理措施）组织应配备数据安全管理审计人员，定期对数据安全管理体系建设、运行过程及相关控制措施进行审计。 |
| | | （管理措施）组织应定期对内部员工数据操作行为进行人工审计。 |
| | | （管理措施）应明确对组织内部数据授权访问、批量复制、开放共享、销毁、数据接口调用等重点环节实施日志留存管理的要求，日志记录至少包括执行时间、操作账号、处理方式、授权情况、IP地址、登录信息等，能够对识别和追溯数据操作和访问行为提供支撑，日志保存时间不少于180天，但法律法规另有规定的除外。 |

表 A.1　数据安全管理体系控制措施（续）

| 控制措施 | | 内容 |
|---|---|---|
| 安全审计 | | （技术措施）应建立针对数据访问和操作的日志监控技术工具，实现对数据异常行为的告警与处置等核心功能。 |
| | | （技术措施）应建立部署数据防泄漏技术手段，具备对不同渠道数据导入导出行为进行监控及对个人信息、重要数据等的外发行为进行告警上报的能力。 |
| 合作方管理 | | （管理措施）组织应建立合作方数据安全管理制度规范，确定数据合作的目标及原则，明确数据合作管理的责任部门和人员、合作方资质能力、合作方监督管理等要求。 |
| | | （管理措施）应明确针对数据合作方的数据安全能力标准规范，根据该规范对数据供应商的数据安全能力进行评估，并将评估结果应用于供应商选择、供应商审核等供应商管理过程中。 |
| | | （管理措施）建立合作方管理台账机制，梳理形成并定期更新合作方清单，清单应至少包括：合作方企业名称、合作业务或系统、合作形式、合作期限、合作方联系人等。 |
| | | （管理措施）应与合作方签订服务合同和安全保密协议，协议应包括但不限于：合作方及项目参与员工可接触到的数据处理相关平台系统范围，及数据使用权限、内容、范围及用途，合作方数据安全责任、保障措施配备情况（保障措施不得低于本企业），合作结束后数据删除要求，合作方违约责任和处罚等。 |
| 应急响应 | | （管理措施）组织应建立数据安全事件管理和应急响应的策略规划，制定数据安全应急响应预案，明确应急响应及应急处置方案。 |
| | | （管理措施）应根据数据安全事件对组织的影响等因素划分事件类型、等级，明确不同类别事件的处置流程和方法，形成相应类型事件的应急预案。 |
| | | （管理措施）应明确应急响应负责人，定期组织开展应急演练活动。 |
| 举报投诉 | | （管理措施）组织应建立数据安全举报投诉与受理机制，明确举报投诉与受理责任部门和人员、处理流程、处理要求等。 |
| | | （管理措施）应建立明确的用户数据安全举报投诉通道，如电子邮件、电话、传真、在线客服等。 |
| | | （管理措施）应建立举报投诉台账，对举报投诉的来源、事件描述、处理过程、处理结果、处理周期等方面进行留档记录。 |
| 数据全生命周期保护 | 数据收集 | （管理措施）组织应制定数据收集管理规范，明确数据收集的原则、渠道、流程、方法、数据格式等要求。 |
| | | （管理措施）利用外部数据源采集数据时，应对数据源的合法合规性进行确认，并定期开展数据收集合规性审查。 |
| | | （管理措施）涉及用户个人信息的采集，应遵循公开透明、最小必要等原则，依据相关法律法规及政策办法的要求，以通俗易懂、简单明了的方式向个人信息主体明示采集规则，如收集、使用个人信息的目的、方式和范围等，并获得个人信息主体的授权同意。 |
| | | （技术措施）应采取技术手段对外部收集的数据和数据源进行识别和记录。 |
| | 数据传输 | （管理措施）组织应建立数据传输安全管理规范，明确数据传输加密场景，形成相应场景下的安全传输策略和操作规程。 |

表 A.1　数据安全管理体系控制措施（续）

| 控制措施 | | 内容 |
|---|---|---|
| 数据全生命周期保护 | 数据传输 | （技术措施）应具备对数据进行加密传输的技术能力，如采用相应的加密算法或安全传输通道（SSL/TLS/IPsec等方式）。 |
| | | （管理措施）传输敏感个人信息时，应依据相关法律法规及组织分类分级原则，对敏感个人信息采取加密等安全措施。 |
| | | （管理措施）应明确组织数据出境业务场景，按照国家数据出境相关管理办法要求执行数据出境安全评估等工作，并留存相关安全评估记录。 |
| | 数据存储 | （管理措施）组织应建立数据存储的安全管理规范，结合数据分类分级策略和管理要求，确定数据存储安全策略和操作规程，明确组织数据存储相关系统平台、存储设备的安全管理规定。 |
| | | （管理措施）组织应建立数据备份与恢复的管理制度，明确数据备份与恢复的操作规程，确定数据备份的周期、方式、地点及恢复验证机制等要求。 |
| | | （管理措施）对授权收集到的敏感个人信息、重要数据、核心数据，应采取加密存储的方式，并且个人信息存储期限应为实现个人信息主体授权使用的目的所需的最短时间。 |
| | | （技术措施）应建立技术手段支撑数据安全存储管理和备份恢复，应具备如配置扫描、身份鉴别、访问控制等能力。 |
| | 数据使用 | （管理措施）组织应结合数据分类分级策略和管理要求，制定不同目的下的数据使用审批流程、数据脱敏处理规则等，明确数据使用的安全策略和操作规程。 |
| | | （管理措施）应建立数据使用的评估制度，涉及敏感个人信息、重要数据及核心数据的使用应先进行安全影响评估，满足国家合规要求后，允许使用。 |
| | | （管理措施）除为达到用户授权同意的使用目的外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。特殊情况下，应告知应用的场景及可能对个人信息主体产生的影响。 |
| | | （管理措施）因业务需要，确需改变个人信息使用目的或改变个人信息使用规则时，应再次征得用户明示同意。 |
| | | （技术措施）应采用技术手段实施数据脱敏，可提供面向不同场景的数据脱敏方案。 |
| | 数据开放共享 | （管理措施）组织应建立数据开放共享管理规范，确定数据开放共享安全策略和操作规程，明确数据开放共享范围、内容与有效控制机制。 |
| | | （管理措施）应建立数据开放共享安全评估机制，确保数据开放共享未超出需求及授权范围。 |
| | | （管理措施）应定期对共享发布的的数据进行审查，确保数据开放共享的合规性。 |
| | | （管理措施）应制定数据接口安全管理规范，明确数据接口的技术控制策略，如身份鉴别、访问控制、授权策略、安全协议等。 |
| | | （管理措施）应与数据开放共享的接口调用方签署合作协议，明确数据的使用目的、供应方式、保密约定、数据安全责任等。 |
| | | （技术措施）应建立技术手段实现对数据接口的认证鉴权与安全监控能力，能够限制违规设备接入，对接口调用进行必要的自动监控和处理。 |
| | 数据销毁 | （管理措施）组织应建立数据销毁管理规范，明确数据销毁场景、销毁对象、销毁方式和销毁流程等要求。 |

表 A.1　数据安全管理体系控制措施（续）

| 控制措施 | | 内容 |
| --- | --- | --- |
| 数据全生命周期保护 | 数据销毁 | （管理措施）组织应建立数据销毁审批机制，设置销毁相关监督角色，监督销毁过程，并对审批和销毁过程进行记录和存档。 |
| | | （技术措施）应配备必要的数据销毁工具和技术手段，确保以不可逆方式实现数据的销毁。 |
| | | （管理措施）应依据国家相关法律法规和管理规定的要求，及时销毁敏感个人信息、重要数据和核心数据。 |

# 参 考 文 献

[1] 《中华人民共和国数据安全法》
[2] 《中华人民共和国个人信息保护法》
[3] GB/T 19000—2016 质量管理体系 基础和术语
[4] GB/T 25069—2010 信息安全技术 术语
[5] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[6] YD/T 3956—2021 电信网和互联网数据安全评估规范
[7] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements

# 电信终端产业协会团体标准

# 数据安全管理体系要求

T/TAF 201—2023

*



电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn